BAB II
DASAR TEORI DAN TINJAUAN PUSTAKA

2.1. Dasar Teori

Dalam penyusunan laporan Tugas Akhir ini dibutuhkan beberapa sumber yang diperlukan untuk dapat lebih memahami teori yang ada dan juga digunakan untuk menunjang kegiatan yang ada. Beberapa dasar teori yang dikemukakan tersebut meliputi konsep dasar dan definisi dari yang akan dikerjakan dan perangkat lunak maupun perangkat *hardware* yang digunakan.

2.1.1. *Information Security*

Information Security atau InfoSec merupakan keamanan informasi berupa data-data yang bersifat sensitif yang ada dalam sebuah instansi. Dalam InfoSec juga terdapat pemahaman mengenai kesadaran keamanan atau *information awareness*. Kesadaran keamanan adalah pengetahuan dan sikap anggota organisasi yang memiliki perlindungan fisik, dan terutama informasi, aset dari organisasi itu.

Sumber Daya Manusia (SDM) dalam suatu instansi haruslah memiliki kesadaran terhadap keamanan informasi. Karena aset dari organisasi tersebut adalah informasi (data-data), teknologi dan SDM. Tidak hanya itu saja, didalamnya juga terdapat aturan dasar dalam menentukan keamanan suatu sistem atau jaringan. Aturan dasar tersebut adalah kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan informasi (*availability*). Menurut Dewanto (2014), *Confidentiality* berguna untuk menjaga kerahasiaan informasi dari orang-orang yang tidak berhak, *Integrity* untuk menjaga perubahan informasi dari orang-orang yang tidak berhak dan *Availability* untuk menjaga agar informasi selalu ada untuk diakses. Ketiga konsep ini sering disebut sebagai *Triad* CIA yang kehadirannya tergantung dari kebutuhan. Pemahaman-pemahaman inilah yang dapat digunakan untuk melakukan *penetration testing*.

Gambar 2. 1 *Triad* CIA

2.1.2. *Penetration Testing*

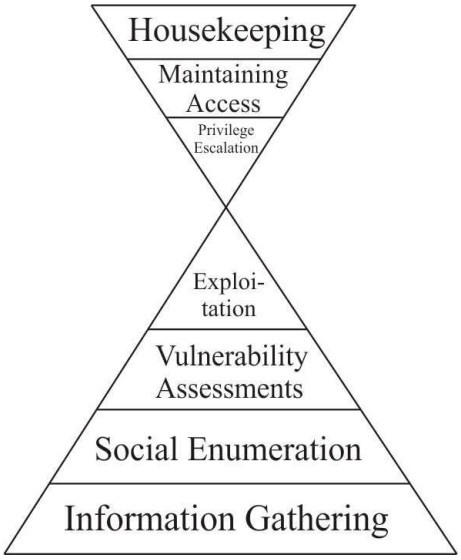
Penetration testing atau dapat disebut *pentesting* adalah suatu kegiatan yang dilakukan seseorang untuk dapat melakukan pegujian untuk menemukan celah keamanan pada suatu sistem yang berpotensi dapat diserang oleh pihak yang tidak bertanggungjawab. Orang yang melakukan *pentesting* adalah *pentester*.

Berikut ini beberapa fase yang biasanya digunakan dalam *penetration testing*:

a. *Information Gathering* merupakan fase yang berguna untuk mendapatkan informasi dari target baik perseorangan maupun perusahaan,
b. *Service Enumeration* merupakan fase pengumpulan informasi yang dilakukan secara aktif bersinggungan dengan target,
c. *Vulnerability Assessments* merupakan fase yang dilakukan untuk mendeteksi, mengidentifikasi, dan mempelajari kelemahan yang terdapat pada suatu target,
d. *Exploitation* merupakan fase yang berguna untuk menyerang suatu target,
e. *Privilege Escalation* merupakan fase untuk meningkatkan hak istimewa untuk mengaksesnya agar pengguna dengan hak akses rendah tidak dapat masuk,

f. *Maintaining Access* merupakan fase untuk mempertahankan akses yang disusupi seperti mengambil sesi yang sudah ada sebelumnya dari ekspolitasi sistem dan layanan web untuk memfasilitasi akses berulang dan eksploitasi lebih lanjut dari sistem komputer dan infrastruktur jaringan yang terpasang, dan

g. *Housekeeping* merupakan fase yang berguna untuk memperbaiki celah pada sistem yang sudah di eksplotasi.



Gambar 2. 2 Fase *Penetration Testing*

2.1.3. Teknik *Information Gathering*

Information Gathering juga biasa disebut sebagai OSINT (*Open Source Intelligence*) yang berarti data yang dikumpulkan dari sumber yang tersedia untuk umum untuk digunakan dalam konteks intelijen. Dalam OSINT terdapat tiga teknik untuk dapat melakukan *Information Gathering* yaitu teknik pasif, teknik semi-pasif dan teknik aktif. Berikut ini penjelasan dari masing-masing teknik.

a. Teknik Aktif

Dalam teknik ini, organisasi yang ditargetkan dapat menjadi sadar akan proses pengintaian yang sedang berlangsung karena *pentester* secara aktif terlibat dengan target. Pengumpulan informasi aktif memerlukan lebih banyak persiapan dari orang yang melakukannya karena meninggalkan jejak, yang kemungkinan akan menyiagakan target atau menghasilkan bukti terhadap dirinya dalam proses penyelidikan digital yang mungkin. Namun, menurut pendapat dominan para ahli di sektor keamanan informasi, proses pengumpulan informasi didasarkan pada gagasan pengintaian pasif yang tujuannya adalah mengumpulkan informasi tentang target hanya melalui sumber daya yang tersedia untuk umum. Oleh karena itu, dua bentuk lainnya dianggap tipikal dari apa yang sebenarnya pengumpulan informasi.

b. Teknik Semi-pasif

Tujuan pengumpulan informasi semi-pasif adalah membuat profil target dengan metode yang akan tampak seperti lalu lintas dan perilaku Internet normal. Kami hanya menanyakan nama *server* yang dipublikasikan untuk informasi, kami tidak melakukan pencarian balik yang mendalam atau permintaan DNS kasar, kami tidak mencari *server* atau direktori "tidak dipublikasikan". Kuncinya di sini adalah tidak menarik perhatian pada aktivitas kita. Post mortem target mungkin dapat kembali dan menemukan kegiatan pengintaian tetapi mereka tidak dapat menghubungkan aktivitas kembali kepada siapa pun.

c. Teknik Pasif

Opsi ini sedang dalam diskusi asalkan ada permintaan eksplisit agar kegiatan pengumpulan tidak terdeteksi oleh target. Dalam hal ini, pentester tidak dapat menggunakan alat yang mengirimkan lalu lintas ke perusahaan yang ditargetkan baik dari

tuan rumahnya maupun yang "anonim" di Internet. Tidak hanya itu akan membebani secara teknis, tetapi juga orang yang melakukan pentest harus membuktikan temuannya dengan apa pun yang dapat dia gali dari informasi yang diarsipkan atau disimpan, yang kadang-kadang tidak mutakhir dan tidak benar karena terbatas pada penyelidikan dikumpulkan dari pihak ketiga.

Dapat diambil kesimpulan bahwa teknik secara pasif merupakan cara untuk mendapatkan informasi yang bisa menggunakan *tools* atau dapat mencari tahu dengan melihat situasi dan kondisi di sekeliling target tanpa diketahui olehnya. Sedangkan teknik secara aktif merupakan cara yang menggunakan *tools* namun langsung mencari informasi target namun beresiko diketahui oleh target. Dalam penelitian ini pun peneliti hanya mengambil salah satu teknik untuk melakukan proses *information gathering*. Ini dikarenakan *information gathering* adalah fase terluas dalam *penetration testing*.

2.1.4. Metode *Penetration Testing*

Selain beberapa fase dalam *pentesting*, terdapat 3 (tiga) metode yang digunakan yaitu *black box*, *gray box* dan *white box*. Berikut ini penjelasan dari masing-masing metode:

a. *White Box*

   White box merupakan metode pengujian yang mendapatkan segala informasi secara penuh yang digunakan dari sistem tersebut seperti teknologi yang digunakan, *source code* yang ada didalamnya, dan lain sebagainya. Dapat disebut berperan sebagai *developer*.

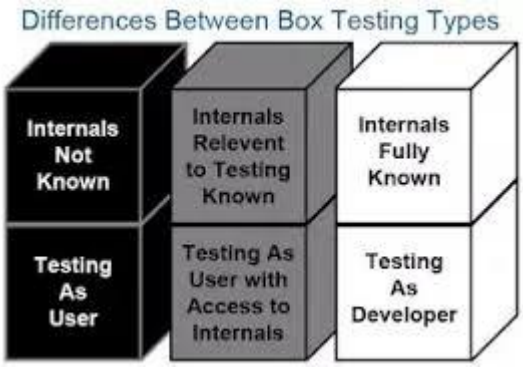
b. *Gray Box*

   Gray box merupakan metode pengujian yang tidak secara penuh mendapatkan informasi didalamnya contohnya hanya diberi

username dan *password* untuk *login*. Metode ini dapat dikatakan berperan sebagai pengguna yang ingin masuk kedalam sistem.

c. *Black Box*

Black box sendiri adalah metode pengujian yang berkebalikan dari *white box*. Jika *white box* mendapatkan secara penuh informasi yang ada pada sistem, maka berbeda dengan *black box* yang sama sekali tidak mendapatkan informasi yang ada dalam sistem tersebut atau bisa disebut sebagai pengguna.



Gambar 2. 3 Perbedaan Metode *Penetration Testing*

2.1.5. *Scanning Tools*

Scanning merupakan tahap yang digunakan untuk mengumpulkan segala informasi target melalui internet menggunakan *tools*. Sedangkan *scanning tools* sendiri merupakan *tools* yang digunakan untuk pemindaian kelemahan pada suatu target. *Tools* yang digunakan beraneka ragam bergantung dari kebutuhan. Berikut ini *tools* yang digunakan dalam penelitian ini:

a. Nmap

Nmap atau *Network Mapper* adalah sebuah *tool* yang digunakan untuk melakukan pemindaian jaringan atau *port scanning*. *Tool* yang dibuat oleh Gordon Lyon ini dapat digunakan untuk meng-audit jaringan yang ada. Dengan

menggunakan *tool* ini pun dapat digunakan untuk melihat *host* yang aktif, *port* yang terbuka, sistem operasi yang digunakan dan lainnya.

b. theHarvester

theHarvester merupakan sebuah *tools* yang dapat digunakan untuk mengummpulkan informasi berupa email, subdomain, host, *employee names*, *open ports* dan lain sebagainya.

c. Maltego

Maltego merupakan perangkat lunak *open source* yang digunakan untuk forensik yang dikembangkan oleh Paterva. Fokus dasar aplikasi ini adalah menganalisis hubungan dunia nyata antara orang, grup, halaman web, domain, jaringan, infrastruktur internet, dan afiliasi dengan layanan online seperti Twitter dan Facebook. Di antara sumber datanya adalah catatan DNS, catatan whois, mesin pencari, jejaring sosial *online*, berbagai API dan berbagai data meta.

2.1.6. DNS Cluster

DNS cluster adalah grup dari *name server* yang memberikan data *record* yang sama untuk domain-domain yang ada dalam grup ini. Setiap domain wajib memiliki minimal dua buah *name server*. Dua buah *name server* ini sebaiknya berada dalam lokasi geografis yang berbeda dan juga *network* yang berbeda. Dengan DNS yang berbeda lokasi geografis dan network ini maka website akan lebih cepat diakses karena pengunjung dapat secara otomatis mencari informasi lokasi web server melalui DNS yang terdekat.

Fungsi lain dari DNS cluster adalah mencegah kegagalan pengiriman email menuju domain yang bersangkutan. Nama lain dari DNS Cluster adalah *load balancing*.

2.1.7. Jenis Pemindaian

Dalam proses ini terdapat tiga jenis *scanning* yang dapat dilakukan untuk melakukan *Information Gathering*, yaitu:

a. Pemindaian port: fase ini melibatkan pemindaian target untuk informasi seperti port terbuka atau tertutup, sistem *live*, dan berbagai layanan yang sedang berjalan.
b. Pemindaian Kerentanan: Memeriksa kelemahan atau kerentanan target yang dapat dieksploitasi. Biasanya dilakukan dengan bantuan alat otomatis.
c. Pemetaan Jaringan: Menemukan topologi jaringan, router, server firewall jika ada, dan meng-host informasi dan menggambar diagram jaringan dengan informasi yang tersedia. Peta ini dapat berfungsi sebagai bagian informasi yang berharga selama proses peretasan.

2.2. Tinjauan Pustaka

Dari peninjauan pustaka yang telah dilakukan oleh peneliti, terdapat beberapa yang memiliki keterkaitan dengan penelitian yang telah dilakukan. Referensi yang digunakan tidak hanya dari skripsi atau tugas akhir yang ada, namun diambil juga dari beberapa buku untuk menambah wawasan peneliti dalam mengerjakan proyek akhir ini.

Diantaranya penelitian dari Irianto (2011) yang berjudul Implementasi Google Hack For Penetration Testing Sebagai Add Ons Google Chrome membahas mengenai bagaimana penerapan *penetration testing* menggunakan Google hack untuk aktifitas *hacking* yang menggunakan Google sebagai medianya dengan bantuan Add Ons Google.

Penelitian dari Suradji dan Chandra (2014) di Rumah Sakit Clara Madiun membahas mengenai keamanan jaringan *server* yang dimiliki institusi tersebut dengan dilakukan *penetration testing* menggunakan metode PTES (*Penetration Testing Executable Standard*) untuk menemukan

kelemahan dari *server* tersebut dengan menggunakan tools Nmap dan Nessus. Karya ilmiah tersebut Penetration Testing Sistem Jaringan Komputer Untuk Mengetahui Kerentanan Keamana Server Dengan Menggunakan Metode *Penetration Testing Execution Standart* (PTES) studi kasus Rumah Sakit Santa Clara Madiun.

Selain itu juga, terdapat penelitian karya ilmiah dari Dewanto (2018) yang membahas mengenai penetration testing terhadap domain uii.ac.id dengan menggunakan metode OWASP Top 10 yang memiliki judul karya ilmiah Penetration Testing Pada Domain uii.ac.id menggunakan OWASP 10.

Selanjutnya penelitian yang diusulkan membahas mengenai penerapan *information gathering* sebagai bagian dari penetration testing terhadap domain akakom.ac.id dengan judul karya ilmiah Implementasi Information Gathering Sebagai Bagian Dari Penetration Testing Terhadap Jaringan STMIK AKAKOM Yogyakarta. Berikut ini tabel penelitiannya:

Tabel 2. 1 Penelitian yang Berhubungan Dengan *Penetration Testing*

Penulis / Parameter	Irianto (2011)	Suradji dan Chandra (2014)	Dewanto (2018)	Fajirulhabshah (diusulkan)
Lokasi	-	RS Santa Clara Madiun	-	STMIK AKAKOM Yogyakarta
Objek	Add Ons Google Chrome	Sistem Jaringan Komputer	uii.ac.id	akakom.ac.id
Standar Industri	-	PTES	OWASP Top 10	-
Vulnerability Scanner/*Tools*	Google Hack	Nmap dan Nessus	The Harvester, Nmap,	Nmap, theHarvester, dan Maltego

			Masscan dan *Web Analisys Scanning*	